Delaware Cyber Security Advisory Council
06/19/2019 09:00 AM
Public Service Commission Conference Room, 861 Silver Lake Blvd., Dover, DE 19904

Meeting Minutes
Printed : 1/2/2020 11:58 AM EST

Delaware Cyber Security Advisory Council (CSAC) Mission Statement

The Delaware Cyber Security Advisory Council is a cross-sector group that explores and promotes best practices to prepare for and prevent cyber security events, makes collaborative recommendations for effective response to such events, and makes recommendations regarding training and resources necessary to drive a culture of cyber preparedness to the citizens, businesses, and organizations that live and operate in the State of Delaware.

Location: Public Service Commission Conference Room, 861 Silver Lake Blvd., Dover, DE 19904

Type of Meeting: CSAC Meeting

Meeting Facilitator: CIO James Collins

Attendees

Present Committee Members

James Collins	Department of Technology and Information (DTI)
Solomon Adote	Department of Technology and Information (DTI)
Nii Attoh-Okine	Delaware State University (DSU)
David Bell	Exelon
Michael Hojnicki	New Castle County Government
Daniel Meadows	Delaware State Police
Georgia Simpson	Middlesex Water Company
Kenneth Kelemen	Courts
Stephen McDonald	Department of Justice
Eric Smith	JP Morgan Chase

Also Present

Claudette Martin-Wus	DTI
George Truitt	DTI
Shelley Turner	DTI
Liam Rafferty	Wilmington University
Jen Coulbourne	DEMEC
Lisa Morris	Department of Justice
Jon Bell	Delaware Better Business Bureau

I. Welcome and Introductions

The meeting commenced at 9:03 a.m.

II. Review and Approval of Last Meeting Minutes

a. The committee reviewed the Committee Meeting minutes from April 17, 2019.

b. Committee members had no revisions or comments. S. Adote made the motion to accept the minutes and J. Christman seconded. The motion was approved.

Motion made by: Solomon Adote
Motion seconded by: Jason Christman
Voting:
Unanimously Approved

III. Chairperson Update

a. J. Collins stated that the State of Delaware has been closely monitoring the $80,000 ransomware attack on Baltimore City which has cost over 10 million dollars in recovery attempts. The floor was opened for comments and sharing regarding the ransomware attack on Baltimore.

b. J. Collins approached the Executive Director for the Delaware League of Local Government in addition to talking to his team regarding Delaware's Cyber Security, how to get the message out and for all to remain vigilant.

c. It is important from an IT perspective that local government hear from individuals outside of local government.

d. A newsletter was sent out to all state employees to remain vigilant.

e. M. Hojnicki suggested hosting an event to help engage local government and the business industry in cyber security awareness talks. As a lot of small businesses are challenge in getting the information and the staff to start good cyber hygiene. These people will need resources and guidance. Cyber security is resource short around the world.

f. S. Adote noted that many entities are securing information insecurely. Statistics show that in 2018 65 % of all small business had been attacked and 60 % did not survive.

g. K. Kelemen mentioned that in addition to the Baltimore attack that the Philadelphia court system has been attacked by malware. This has been going on for weeks and is in parallel to what is going on in Baltimore.

h. J. Collins explained that the reason for discussing this is to help better determine what to focus on and our strategy, but the bottom line is we need good cyber hygiene and that starts with the basics.

IV. Public Comment

a. J. Collins opened the floor for public comment.

b. Jon Bell of Delaware Better Business Bureau (BBB) introduced himself and explained his role at the Better Business Bureau. The agency is a non-profit agency. He deals with a lot fraud and social engineering. His agency tries to do outreach with both the public and business. Although, in his opinion most businesses are too small to adopt good cyber hygiene practices. He is interested in

hearing ideas that educate/motivate small businesses and how this council is going to engage with small businesses. Delaware Better Business tracks all businesses that it can collect data on. The agency also does education with the public, compile and research reports so that they can identify what is happening here in Delaware. Using examples close to home. They share case studies and workshops to encourage people to be safe and to aid in making businesses safe. Outreach focuses on one on one and local workshops as education is the only way to prevent cyber-attacks.

c. Jen Coulbourne– formed an IT working group with local municipalities and puts them in touch with local resources. They meet quarterly. She has been working with Sandee Alexander as her focus group is concentrating on disaster recovery. The focus groups topic for July is supply chain risk management.

d. J. Collins thanked everyone for working with the local municipalities.

e. S. Adote stressed the need that one of our agenda items be cyber risk.

f. M. Hojnicki stated that cyber risk is a target for the Fall as some level of cyber security training or self-assessment is starting to be required for applying for federal grants.

g. AJ Schall will be working with Solomon and Claudette to ensure our compliance.

V. Review Last Strategic Session Results

a. S. Adote reviewed the input from the members from the previous meeting's strategic planning activity that would be built upon at the current meeting.

VI. Strategic Plan Development Activity

Discussion

a. J. Collins advised each committee member that the form they have been given is the output from their last strategic session and that the information had been broken down into 3 categories.

b. S. Adote noted that the committee needs to focus on the products coming out of this strategy and the value to the local government. We know the core work stream and core values. It was advised that the committee start with training and best practices, these are areas that we can put resources into now.

c. E. Smith suggested that cybersecurity training be offered quarterly with a more elaborate yearly training.

d. S. Adote recommended training through webinars.

e. J. Collins suggested micro learning as it is an excellent way to engage. This committee does not need to create courses. There may be courses that already exist. We can bring in speakers from specialized areas to talk about cyber items like NIST.

f. Committee members were given index cards and asked to select 3 topics for discussion.

1. S. Adote discussed if a separate guide for small business should be developed or develop a standard that can be shared with all entities.
2. D. Bell discussed the mission statement and how adopting the cloud is the best solution as backups are important and cloud offers many different types of backups. Small businesses may need to outsource their IT.
3. J. Collins discussed internships and the need to write for grants for funding to pay interns.

4. S. Adote asked if there were any services that would allow small businesses or utilities to access and/or share data breach information.
5. D. Meadows advised that the information would first have to be disseminated.
6. J. Collins explained that good practices will reduce the risk of attacks. We need to focus on those basic cyber threats so that we will become more immune to threats.
7. We are evolving as IT people from being in the engine room to being on the bridge. We need to highlight the IT folks and bring awareness to get funding.

g. J. Collins stated that we are now having conversations and letting our agencies know that they will need to take steps to protect/shield their apps.

Actions/Next Steps to Build on those topics

a. A. Schall questioned whether we should purchase cyber insurance.

b. M. Hojnicki explained that there is a legal aspect we must look at and legal review would be needed. It will be a learning experience if cyber insurance is purchased.

c. D. Bell explained that cyber insurance can be very good if you have direct cost. You can highlight specific things that you want to insure.

d. J. Collins asked that cyber insurance be an item on our next agenda and noted that cyber insurance can be voided if an agency is not using good cyber hygiene.

Better understanding of what is needed

a. S. Adote commented on incident response framework as part of standards and good practices. We need to share information on what you can do to respond to an incident whether you are a citizen or a small business.

b. M. Hojnicki suggested that there be a number to call whether you are a citizen or a business that will get them to the first step.

c. S. Adote explained how our participation in last weeks tabletop brought a lot of issues to light such as identifying the event; identifying the process and how to narrow it down and when to contact the federal government. DSHS is there to help you recover and the FBI is more the defensive arm.

d. D. Meadows advised that they have trained taskforce offers that can start to pursue criminal events.

VII. Old Business

a. C. Martin-Wus reminded attendees about the FEMA Region III Meeting and Workshop and to sign-up if they had not done so. FEMA Region III Meeting and Workshop will include participation from multiple States. This will allow us to better see what is occurring regarding incidents, how they are being dealt with, create partnerships and networks that will allow communications and information sharing within and our State and other States.

b. S. Adote communicated to the committee that he, Daniel Meadows, and Eric Smith had a chance to review the mission statement. The mission statement was shared with the committee. Mission Statement captures essence:

“The Delaware Cyber Security Advisory Council is a cross-sector group that explores and promotes best practices to prepare for and prevent cyber security events, makes collaborative recommendations for effective response to such events, and

makes recommendations regarding training and resources necessary to drive a culture of cyber preparedness to the citizens, businesses, and organizations that live and operate in the State of Delaware."

VIII. Adjourn

a. J. Collins thanked all attendees. The meeting was adjourned at 10:58 a.m.

_____ _____

\- -